CLAIMS

.Please amend the claims as follows:

1.   (currently amended) A method in a data processing system for maintaining security during booting of the data processing system, said method comprising:
    during a boot process, interrogating a boot device for password information; and
    in response to the boot device supplying ~~password information~~ a device password corresponding to that of a trusted boot device, booting the data processing system utilizing the boot device, wherein said booting comprises booting the data processing system utilizing the boot device without entry of any of said ~~password information~~ device password corresponding to that of a trusted boot device by a human user.

2.   (currently amended) The method according to Claim 1, wherein said ~~password information~~ device password includes at least a serial number of the boot device.

3.   (currently amended) The method according to Claim 1, wherein interrogating said boot device for ~~password information~~ said device password comprises startup software interrogating the boot device.

4.   (currently amended) The method according to Claim 1, wherein interrogating said boot devices for ~~password information~~ said device password comprises interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies ~~password information~~ said device password corresponding to that of a trusted boot device.

5.   (currently amended) The method according to Claim 1, and further comprising:
    storing a password in non-volatile storage of the data processing system; and
    determining that said boot device has supplied ~~password information~~ said device password corresponding to a trusted boot device by hashing ~~password information~~ said

device password supplied by the boot device and comparing the hashed ~~password information~~ device password with the stored password.

6.   (currently amended)   The method according to Claim 5, and further comprising obtaining said password by interrogating the boot device for ~~the password information~~ said device password with a password-protected configuration routine.

7.   (currently amended)   Data processing system comprising:
a boot device;
a processor; and
memory coupled to said processor for communication, said memory including startup software that, when executed by said processor during a boot process, interrogates the boot device for ~~password information~~ a device password and, responsive to the boot device supplying ~~password information~~ said device password corresponding to that of a trusted boot device, boots the data processing system utilizing the boot device, wherein said startup software boots the data processing system utilizing the boot device without entry of any of said ~~password information~~ device password corresponding to that of a trusted boot device by a human user.

8.   (currently amended)   The data processing system of Claim 7, wherein said ~~password information~~ device password includes at least a serial number of the boot device.

9.   (currently amended)   The data processing system of Claim 7, said data processing system having a plurality of boot devices including the boot device, wherein said startup software interrogates said plurality of boot devices for ~~password information~~ said device password in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device.

10.   (currently amended)   The data processing system of Claim 7, and further comprising non-volatile storage that stores a password, wherein said startup software

determines that said boot device has supplied ~~password information~~ said device password corresponding to a trusted boot device by hashing ~~password information~~ said device password supplied by the boot device and comparing the hashed ~~password information~~ device password with the password stored in non-volatile storage.

11.   (currently amended) The data processing system of Claim 10, said startup software including a password-protected configuration routine that obtains said password by interrogating the boot device for ~~the password information~~ said device password.

12.   (currently amended)   A program product comprising:
    a computer usable medium; and
    startup software encoded within said computer usable medium, wherein said startup software causes a data processing system to interrogate the boot device for ~~password information~~ a device password during a boot process and, responsive to the boot device supplying ~~password information~~ said device password corresponding to that of a trusted boot device, to boot the data processing system utilizing the boot device, wherein said startup software boots the data processing system utilizing the boot device without entry of any of said ~~password information~~ device password corresponding to that of a trusted boot device by a human user.

13.   (currently amended)   The program product of Claim 12, wherein said ~~password information~~ device password includes at least a serial number of the boot device.

14.   (currently amended)   The program product of Claim 12, said data processing system having a plurality of boot devices including the boot device, wherein said startup software causes the data processing system to interrogate said plurality of boot devices for ~~password information~~ said device password in sequence according to a priority order until a boot device supplies ~~password information~~ said device password corresponding to that of a trusted boot device.

15.   (currently amended) The program product of Claim 12, wherein said startup software determines that said boot device has supplied ~~password information~~ said device password corresponding to a trusted boot device by hashing ~~password information~~ said device password supplied by the boot device and comparing the hashed ~~password information~~ device password with a password stored in non-volatile storage of the data processing system.

16.   (currently amended) The program product of Claim 15, said startup software including a password-protected configuration routine that obtains said password by interrogating the boot device for the ~~password information~~ said device password.

17.-19. (canceled)